UNITED STATES DISTRICT COURT

for the

Middle District of North Carolina

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

3845 Eastview Drive,
Winston-Salem, North Carolina 27107

Case No. 1:21MJ167-1

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A, attached hereto and made a part of.

located in the Middle District of North Carolina, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, attached hereto and made a part of.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 2252A(a)(5)(B)	Possession of Child Pornography
18 U.S.C. § 2252A(a)(2)(A)	Distribution of Child Pornography

The application is based on these facts:

Please see the attached affidavit.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/S/ Tara S. Thomas
Applicant's signature

Tara S. Thomas, FBI Special Agent
Printed name and title

On this day, the applicant appeared before me via reliable electronic means, that is by telephone, was placed under oath, and attested to the contents of this Application for a search warrant in accordance with the requirements of Fed. R. Crim. P. 4.1.

Date: 05/11/2021 12:45pm

Judge's signature

City and state: Durham, North Carolina

Joe L. Webster, United States Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Tara S. Thomas, a Special Agent with the Federal Bureau of Investigation, being duly sworn, depose and state as follows:

INTRODUCTION

1. I am investigating offenses related to child sexual exploitation. This Affidavit is submitted in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises located at 3845 Eastview Drive, Winston-Salem, North Carolina 27107 (the "SUBJECT PREMISES"), more specifically described in Attachment A, for contraband and evidence, fruits, and instrumentalities of violations of Title 18 U.S.C. §§ 2252A(a)(2)(A) and 2252A(a)(5)(B), which items are more specifically described in Attachment B.

2. The statements in this Affidavit are based in part on information provided by other law enforcement officers and on my investigation of this matter. Since this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that contraband and evidence, fruits, and instrumentalities of violations of Title 18 U.S.C. §§

2252A(a)(2)(A) and 2252A(a)(5)(B) are presently located at the SUBJECT PREMISES described in Attachment A.

AFFIANT BACKGROUND

3. I am a Special Agent of the Federal Bureau of Investigation ("FBI"), and have been since March of 2008. My initial training consisted of a twenty-week FBI new agent course during which I received instruction on various aspects of federal investigations, ranging from economic espionage and child pornography, to kidnapping and computer intrusions. Prior to joining the FBI, I worked in law enforcement for over eight years as a police officer and sheriff's investigator. I am currently assigned to the Charlotte Division and stationed at the Greensboro Resident Agency.

4. I have supported numerous FBI investigations through investigative research and analysis, to include investigations of cybercrime. I am familiar with, and have employed, investigative techniques used in these investigations, such as analysis of Internet Protocol addresses and Internet Service Provider records. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. § 2252A, and I am authorized by law to request a search warrant. As a Special Agent, I am

authorized to investigate violations of laws and to execute warrants issued under the authority of the United States.

STATUTORY AUTHORITY

5. As noted above, this investigation concerns alleged violations of the following:

a. 18 U.S.C. § 2252A(a)(2)(A) prohibits a person from knowingly receiving or distributing child pornography, as defined in 18 U.S.C. § 2256(8), using any means and facility of interstate and foreign commerce, that has been mailed, or that has been shipped and transported in and affecting interstate and foreign commerce by any means, including by computer. Attempts and conspiracies are also violations of this statute.

b. 18 U.S.C. § 2252A(a)(5)(B) prohibits a person from knowingly possessing or knowingly accessing with intent to view any material that contains an image of child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed or shipped or

transported in or affecting interstate or foreign commerce by any means, including by computer. Attempts and conspiracies are also violations of this statute.

DEFINITIONS

6. The following definitions apply to this Affidavit and Attachments:

a. "Chat," as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

b. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.

c. "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit

conduct, where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

d. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, other mobile phones, and other mobile devices. *See* 18 U.S.C. § 1030(e)(1).

e. "Computer hardware," as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives,

"thumb," "jump," or "flash" drives, which are small devices that are plugged into a port on the computer, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

f. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

g. "Geolocated," as used herein, refers to the identification of the geographical location of (a person or device) by means of digital information processed via the Internet.

h. "Hashtag," as used herein, refers to a word or phrase preceded by a hash or pound sign (#), which is used to identify messages or groups on a specific topic.

i. A "Hash value" is a unique multi-character number that is associated with a computer file. Some computer scientists compare a hash value to an electronic fingerprint in that each file has a unique hash value. Any identical copy of the file will have exactly the same hash value as the original, but any alteration of the file, including even a change of one or two pixels, would result in a different hash value. Hash values represent large amounts of data as much smaller numeric values, so they are used with digital signatures.

j. "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email,

remote storage, and co-location of computers and other communications equipment.

k. An "Internet Protocol address" or "IP address," as used herein, refers to a unique numeric or alphanumeric string used by a computer or other digital device to access the Internet. Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most Internet Service Providers ("ISPs") control a range of IP addresses. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

l. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet

often cross state and international borders, even when the devices communicating with each other are in the same state.

m. "Minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

n. "Mobile application" or "chat application," as used herein, are small, specialized programs downloaded onto mobile devices, computers and other digital devices that enable users to perform a variety of functions, including engaging in online chat and sending or receiving images and videos.

o. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

p. "Remote computing service", as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

q. "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons

of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the anus, genitals, or pubic area of any person.

r. A "storage medium" is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, "thumb," "jump," or "flash" drives, CD-ROMs, and other magnetic or optical media.

s. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

BACKGROUND ON KIK MESSENGER AND DROPBOX

7. Kik Messenger (hereinafter "Kik") is a mobile application designed for chatting or messaging owned and operated by MediaLab.AI, Inc., a United States based holding company of Internet brands. Kik was formerly owned by Kik Interactive, Inc., a Canadian based company. MediaLab.AI, Inc., acquired the Kik application in October 2019.

8. According to "Kik's Guide for Law Enforcement," last revised in February 2020, to use the Kik application, a user downloads the application to a mobile phone, computer, or other digital device via a service such as the iOS App Store, Google Play Store, Apple iTunes, or another similar provider. Once the application is downloaded and installed, the user is prompted to create an account and username. The user is asked to supply an email address; however, the email address does not have to be verified in order to use the application. The user also creates a display name, which is a name that other users see when transmitting messages back and forth. Once the user has created an account, the user is able to locate other users via a search feature. While messaging, users can then send each other text messages, images, and videos.

9. According to "Kik's Guide for Law Enforcement," Kik users are also able to create chat groups with a limited number of individuals to communicate in a group setting and exchange text messages, images and videos. These groups are administered by the group creator who has the authority to remove and ban other users from the created group. Once the group is created, Kik users have the option of sharing a link to the group that includes all of their contacts or any other user. These groups are frequently

created with a group name containing a hashtag (#) that is easily identifiable or searchable by keyword.

10. Dropbox is a personal cloud storage service (sometimes referred to as an online backup service) that is frequently used for file storage, syncing, sharing, and content collaboration. The Dropbox application is available for Windows, Macintosh and Linux desktop operating systems. There are also apps for Apple and Android devices. The service provides 2 gigabytes (GB) of storage for free, with multiple other fee options.

PROBABLE CAUSE

11. On November 11, 2018, a Cybertip from the National Center for Missing and Exploited Children (NCMEC) was assigned to Kernersville Police Department (KPD). The information in the Cybertip was a collection of child pornography being maintained in the Dropbox account using the email address **kickassman420@gmail.com** with the screen name "Adam Shelton". The investigation by KPD is summarized here:

a. On September 11, 2018, Dropbox reported the account associated with **kickassman420@gmail.com** as containing child pornography and sent associated files to NCMEC.

b. The NC State Bureau of Investigation received the Cybertip. On October 17, 2018, Charter responded to a subpoena regarding the IP address 2606:a000:824d:a100:4c29:ed63:b107:c7ae, the last IP address accessing the Dropbox account. The IP address was registered to Sereika Sydney of 342 South Cherry Street, Apartment B, Kernersville, NC 27284. The email associated with the account was **kickassman420@gmail.com**.

c. On November 1, 2018, KPD received the Cybertip from NCSBI. Internal KPD and publicly available database checks confirmed that Sydney and Adam Wayne SHELTON (the "SUBJECT PERSON" or "SHELTON") were residing together at the time.

d. On January 30, 2019, Dropbox responded to a search warrant regarding the account associated with **kickassman420@gmail.com.** The account contained over 170 videos deemed child pornography.

12. On February 16, 2019, KPD requested FBI assistance as it appeared SHELTON had moved to Greensboro, NC. I accepted the investigation. I reviewed the Dropbox account associated with

kickassman420@gmail.com. The following is a summary of two of the videos found in the account:

a. A video entitled "!(~pthc_center~)(opva)(2014)_marys_pussy_and_ass_6yr_girl_sweet.avi.vid[1] " depicts a prepubescent female child, approximately six years old, with brown hair and sunglasses. Her shirt was pulled up to expose her nipples, and her pants were pulled down to her ankles. The video shows her genitals in multiple settings and an adult male is seen manipulating her genitals and touching her vagina with his fingers. The video is approximately 1 minute and 2 seconds long.

b. A video entitled "Daphne 8yo plenity sex pleasure (childlover xxxxx)part 3" depicts a prepubescent female child, approximately eight years old, with long braided blonde hair. She is completely nude and interacts with an adult male. She provides manual stimulation to the adult male's penis, and she climbs on top of the male and inserts his penis in her vagina. The adult male then gets on top of the child and inserts his penis in the child's vagina. The video is approximately 6 minutes and 14 seconds long.

13. Publicly available database checks were conducted, and it appeared SHELTON had moved to Illinois. The case was placed on hold.

14. In November of 2020, I was working on closing out historical cases from my case load and began working on this case again. On December 1, 2020, I interviewed Shirley May Shelton at her residence at 3521 McKnight Mill Road, Greensboro, NC 27405. She confirmed she is SHELTON's grandmother. She indicated that SHELTON used to live with her but moved to Illinois last year or the year before. She said SHELTON moved back to North Carolina recently and now lives with his mother in Winston-Salem, NC.

15. On December 1, 2020, I spoke with Lisa Bracken, the mother of SHELTON. She confirmed that SHELTON is living with her along with his 10-month-old daughter at 3845 Eastview Drive, Winston-Salem, North Carolina 27107 (the "SUBJECT PREMISES") and is currently employed by Matcor Metal Fabrication in Lexington, NC. I requested Bracken have her son call me. SHELTON called me that afternoon, refused an interview multiple times, and asked if he needed an attorney. I told him that was his own decision. I asked him to call me back once he made a decision.

16. December 1, 2020, Nils Gerber, a Winston-Salem criminal attorney, called me and advised SHELTON had retained him regarding this

federal investigation. On December 2, 2020, FBI Task Force Officer Tommy Hyatt and I met with SHELTON's attorney while SHELTON waited in the lobby. Due to the historical nature of SHELTON's alleged criminal activity in 2018, a federal search warrant would not have been feasible at the time. After being offered the opportunity to turn over SHELTON's devices to check for child pornography and have any that contained child pornography be wiped and returned without any federal prosecution, Gerber declined on behalf of his client. Gerber acknowledged that turning over SHELTON's devices was not in the best interest of his client. TFO Hyatt and I advised SHELTON, in the presence of Gerber, not to destroy any evidence in his possession. I advised SHELTON and his attorney that the investigation into SHELTON would continue, and if SHELTON did obstruct justice in any way during the investigation he would be prosecuted.

17. I worked on the investigation further by submitting subpoenas to Google and Charter, but no new information was garnered. The case was placed on hold again.

18. On April 29, 2021, I was advised by an FBI agent from the Springfield Division of another open case into SHELTON. A Kik user named "**mr.bearrxxx**", subsequently identified as SHELTON, had distributed child

pornography within a group on Kik that was established as dedicated to the trade of child pornography. An online covert employee (OCE) from the Winnebago County Sheriff's Office (WCSO) was able to download two images from **mr.bearxxx** that were deemed child pornography. The investigation is summarized here:

a. On June 10, 2020, an OCE from WCSO accessed multiple Kik chat groups dedicated to child pornography. One of these groups was named "private group 3.14 (anything goes)". The user **mr.bearxxx** was a member of this group. Over the course of time spent within this group multiple images and videos of child pornography have been shared with members of the group. Within this group, the user identified above would have had access to multiple images and videos depicting child pornography as a member of the group. The user **mr.bearxxx** sent out images and videos depicting child pornography. Two of the images are described below:

1) Video entitled "IMG_2149.mp4" depicts a nude prepubescent female child approximately 5 to 7 years old lying on her back with her vagina exposed. An adult male can be seen inserting his finger into the prepubescent females exposed vagina. The

video is one minute and three seconds long. This video was sent on June 10, 2020.

2) Image entitled "IMG_2155.jpg" depicts a prepubescent female child approximately 6 to 8 years old with seven adult erect penises around her face. Based on my training and experience, some of the adult penises appear to be photoshopped into the image. However, at least two appear to actually be in the room with the child and at least one adult male is ejaculating on the child. This image was sent on June 10, 2020.

b. On July 21, 2020, Kik responded to a subpoena regarding the Kik user **mr.bearxxx**. The account is linked to the Gmail address sheltonadam50@gmail.com, a confirmed address meaning the address was accessed to confirm the Kik account. The Kik account was accessed by an Android LG cell phone and was created on March 20, 2020.

c. On September 9, 2020, CTI, an ISP in Illinois, responded to a subpoena regarding the IP address 160.32.230.206, the last IP address accessing the Kik account on July 9, 2020. The IP address was registered to Adam Shelton, address 605 East Vine, Taylorville, IL 62568, email

address sheltonadam50@gmail.com, and cell phone number 217-561-3531. The account with CTI was created on February 28, 2020.

d. On September 14, 2020, Google responded to a subpoena regarding the email address sheltonadam50@gmail.com. The email was created on October 19, 2018. The recovery SMS and sign-in phone number was listed as 217-561-3531, SHELTON's cell phone number.

19. Due to SHELTON having an infant daughter, I reviewed the material I received regarding the Kik information. The children depicted in the two images were not his daughter.

20. On April 29, 2021, surveillance observed the residence located at the SUBJECT PREMISES, 3845 Eastview Drive, Winston-Salem, North Carolina 27107. The residence is described as a brick single-story home with black shutters and a carport to the left of the front door when facing it from the street. The numbers "3845" are over the front door as well as on the mailbox. The property is listed in Davidson County Tax Records as parcel number 01003A0000088 and PIN 6863-0300-6382 belonging to Kenneth and Lisa Bracken.

21. A check of publicly available databases showed the SUBJECT PERSON, Adam Wayne SHELTON, date of birth 10/22/1986, and Lisa Bracken, date of birth 09/16/1965, live at the SUBJECT PREMISES.

22. On May 5, 2021, and multiple other dates, I observed vehicles at the SUBJECT PREMISES registered to Lisa Bracken, SHELTON's mother.

23. On May 5, 2021, I observed SHELTON operating a vehicle registered to him under Illinois Department of Motor Vehicles bearing license plate 588123, a silver Chevrolet Impala ("SUBJECT VEHICLE"). SHELTON drove to Matcor Metal Fabrication, 835 Salem Road, Lexington, NC 27295. SHELTON walked into the business.

24. Based on my training and experience, it is probable that SHELTON has built and maintained a collection of child pornography, which is kept where it is secure and readily accessible at the SUBJECT PREMISES and/or on the SUBJECT PERSON and/or in the SUBJECT VEHICLE. Due to the nature of SHELTON's employment, a metal fabrication warehouse, it may be against company policy to bring a cell phone into the business. Therefore, SHELTON may leave his cell phone in the car when he goes to work.

25. Based on the facts listed above, there is probable cause to believe that there is evidence of a continual pattern of on-going possession of child

pornography, in violation of Title 18 U.S.C. § 2252A(a)(5)(B), and distribution of child pornography, in violation of 18 U.S.C. § 2252A(a)(2)(A), located at the SUBJECT PREMISES.

BACKGROUND ON CHILD PORNOGRAPHY, COMPUTERS, AND THE INTERNET

26. I have had both training and experience in the investigation of computer-related crimes, as well as that of other agents assisting in the investigation. Based on my training, experience, and knowledge, I know the following:

a. Computers and digital technology are the primary way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

b. Digital cameras and computers with cameras save photographs or videos as a digital file that can be directly transferred to a computer by connecting the camera or smartphone to the computer, using a cable or via wireless connections such as "WiFi" or "Bluetooth." Photos and videos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These

memory cards are often large enough to store thousands of high-resolution photographs or videos.

c. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Mobile devices such as smartphones and tablet computers may also connect to other computers via wireless connections. Electronic contact can be made to literally millions of computers around the world. Child pornography can therefore be easily, inexpensively and anonymously (through electronic communications) produced, distributed, and received by anyone with access to a computer or smartphone.

d. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. Electronic storage media of various types - to include computer hard drives, external hard drives, CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices that are plugged into a port on the computer - can store thousands of images or videos at very high resolution. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a

computer, and then copy it (or any other files on the computer) to any one of those media storage devices. Some media storage devices can easily be concealed and carried on an individual's person. Smartphones and/or mobile phones are also often carried on an individual's person.

e. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

f. Individuals also use online resources to retrieve and store child pornography. Some online services allow a user to set up an account with a remote computing service that may provide email services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account (sometimes referred to as "cloud" storage) from any computer or smartphone with access to the Internet. Such an account can also be accessed in the same way. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer, smartphone, or external media in most cases.

g. A growing phenomenon related to smartphones and other mobile computing devices is the use of mobile applications, also referred

to as "apps." Apps consist of software downloaded onto mobile devices that enable users to perform a variety of tasks – such as engaging in online chat, sharing digital files, reading a book, or playing a game – on a mobile device. Individuals commonly use such apps to receive, store, distribute, and advertise child pornography, to interact directly with other like-minded offenders or with potential minor victims, and to access cloud-storage services where child pornography may be stored

h. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional (*i.e.*, by saving an email as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files) or unintentional. Digital information, such as the traces of the path of an electronic communication, may also be automatically stored in many places (*e.g.*, temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

i. Individuals involved in the receipt, possession, and/or distribution of child pornography very frequently possess multiple devices that contain evidence of their interaction with child pornography and/or sexual interest in minors. In modern American culture, most individuals possess multiple devices that have the ability to connect to the Internet (e.g., tablets, desktop computers, laptop computers, and mobile phones). Many individuals also keep prior versions of their devices (e.g., prior cell phones and prior computers). This is the case because (1) individuals are often reluctant to discard devices that frequently contain significant personal information and (2) current devices may malfunction and prior versions can often be used until the current device is repaired or replaced.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

27. As described above and in Attachment B, this application seeks permission to search for records that might be found at the SUBJECT PREMISES, in whatever form they are found. One form in which the records are likely to be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic

storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

28. I submit that if a computer or storage medium is found at the SUBJECT PREMISES, there is probable cause to believe those records referenced above will be stored on that computer or storage medium, for at least the following reasons:

a. Deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

b. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear;

rather, that data remains on the storage medium until it is overwritten by new data.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

29. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used

them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium at the SUBJECT PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. Information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus

enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (*e.g.*, registry information, communications, images and movies, transactional information, records of session times and durations, Internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, computers typically contain information that logs: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the Internet. Such information allows investigators to

understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (*e.g.*, a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (*e.g.*, Internet searches indicating criminal planning), or consciousness of guilt (*e.g.*, running a "wiping" program to destroy evidence on the computer or password

protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For

example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to obtain or access child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

30. Based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices, including external and internal hard drives, flash drives, thumb

drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to "cloud" storage. I also know that during the search of the premises it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:

a. Searching computer systems is a highly technical process that requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software, or operating system that is being searched;

b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted, or password-protected data. Computer hardware and storage devices may

contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted.

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises; and

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, computer users can

conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is contraband, evidence, fruits, or instrumentalities of a crime.

31. Additionally, based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that routers, modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of wireless routers, which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be secured (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or unsecured (in that an individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as

the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know that individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

32. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

CONCLUSION

33. Based on the foregoing, there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that the contraband, property, evidence, fruits and instrumentalities of these offenses,

more fully described in Attachment B, are located at the premises described in Attachment A. I, therefore, respectfully request that the attached warrant be issued authorizing the search of the SUBJECT PREMISES described in Attachment A, and the seizure of the items listed in Attachment B.

/S/ Tara S. Thomas
Special Agent
Federal Bureau of Investigation

Dated: May 11, 2021 12:45pm

Pursuant to Rule 4.1 of the Federal Rules of Criminal Procedure, the affiant appeared before me via reliable electronic means (telephone), was placed under oath, and attested to the contents of this written affidavit.

THE HONORABLE JOE L. WEBSTER
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

DESCRIPTION OF LOCATION TO BE SEARCHED

The entire premises located at 3845 Eastview Drive, Winston-Salem, North Carolina 27107. The residence is described as a brick single-story home with black shutters and a carport to the left of the front door when facing it from the street. The numbers "3845" are over the front door as well as on the mailbox. The property is listed in Davidson County Tax Records as parcel number 01003A0000088 and PIN 6863-0300-6382 belonging to Kenneth and Lisa Bracken.

ATTACHMENT B

ITEMS TO BE SEIZED

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of 18 U.S.C. §§ 2252A(a)(2)(A) and 2252A(a)(5)(B):

1. Computers or storage media that could be used as a means to commit the violations described above, and on which the things described in this warrant could be stored.
2. Routers, modems, and network equipment used to connect computers to the Internet.
3. Child pornography, as defined in 18 U.S.C. 2256(8).
4. Child erotica.
5. Records, information, and items relating to violations of the statutes described above in the form of:
    a. Records and information referencing child pornography, as defined in 18 U.S.C. 2256(8), and/or child erotica;
    b. Records, information, and items referencing or revealing the occupancy or ownership of 3845 Eastview Drive, Winston-Salem, NC 27, including utility and telephone bills, mail envelopes, or addressed correspondence;
    c. Records and information referencing or revealing access to Dropbox or the Google emails kickassman420@gmail.com or sheltonadam50@gmail.com;

d. Records and information referencing or revealing access to and/or use of Kik Messenger;

e. Records and information referencing or revealing the use of the handle "mr.bearxxx," or any variant thereof, and the identity of the user;

f. Records and information referencing or revealing the owner or user of an Android at the SUBJECT PREMISES;

g. Records and information referencing or revealing the trafficking, advertising, or possession of child pornography, to include the identity of the individuals involved and location of occurrence;

h. Records and information referencing or revealing a sexual interest in children or the sexual exploitation of children, to include the identity of the individuals involved and location of occurrence such as social media sites or applications containing groups or chat rooms dedicated to accessing child pornography, to include Kik, and Facebook, as well as online repositories known to be accessed with the intent to view child pornography such as Imjur and TOR;

i. Records and information referencing or revealing the use of remote computing services such as email, cloud storage, or online social media services; and

j. Records and information referencing minors and/or revealing their identities.

6. For any computer or storage medium whose seizure is otherwise authorized by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, deleted, viewed, or otherwise interacted with;

b. evidence of how and when the COMPUTER was used to create, edit, delete, view, or otherwise interact with or access child pornography or share child pornography with others;

c. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

d. evidence of the Internet Protocol addresses used by the COMPUTER;

e. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

f. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

g. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

h. evidence of the lack of such malicious software;

i. evidence of programs (and associated data) that are designed to eliminate data from the COMPUTER;

7. During the course of the search, photographs of the location to be searched may be taken to record the condition thereof and/or the location of items therein.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form

(such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact discs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.